The Survivable Network Analysis Method:

Assessing Survivability of Critical Systems

CERT/Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Sponsored by the U.S. Department of Defense

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JAN 2004**	2. REPORT TYPE	3. DATES COVERED **00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE
The Survivable Network Analysis Method: Assessing Survivability of Critical Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**20**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Mission Survivability

Changing Environment

- System Evolution
  - expanding network boundaries
  - additional participants with varying levels of trust
  - numerous point solutions: Public Key Infrastructure, Virtual Private Networks, Firewalls
  - blurring of Intranet and Extranet boundaries
  - new technologies -- directory services, XML
- The impact of attacks is on organizations, and hence on the applications which support the organization’s mission

Impact on Analysis

- Lack of complete information
  - physical and logical perimeters
  - participants, untrusted insiders
  - software components --- COTS Java, etc.
- Mix of central and local administrative control
- Critical components more exposed
- An attack could impact essential business services

Survivability Defined

Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

Key properties

- Mission Focus
  - Identification of risks and trade-offs
  - Alternative means to meet mission
- Assume imperfect defenses

The "Three Rs"

- *Resistance*
  - Capability to deter attacks
- *Recognition*
  - Capability to recognize attacks and extent of damage
- *Recovery*
  - Capability to provide essential services/assets during attack and recover full services after attack

Techniques and Methods

- Traditional Security
  - fortress model: firewalls, protection, security policy
  - insider trust
  - encryption, authentication, passwords
  - resistance and recognition with recovery secondary

- Survivability is enhanced by
  - security techniques where applicable
  - redundancy, diversity, general trust validation, etc
  - automated recovery support

Example

- E-mail
  - E-mail content tunnels through firewalls
  - Always time lag between initial discovery and upgraded virus signatures required for scans
  - Enhanced e-mail functionality
    - Attachments (Word macros)
    - Rich content such as HTML, Javascript
  - Resistance and recognition limited. Recovery strategies essential.
  - Significant impact on services other than e-mail.

The Survivable Network Analysis Method

- Focus
  - early phase of life cycle
  - applications as well as system infrastructure
  - tailorable depending on stage of development.

- Three options for SNA analysis
  - survivability architecture
  - survivability requirements
  - mission lifecycle

Architectural Focus

- Capture assumptions such as boundaries and users
- Support system evolution as requirements and technologies change
  - evolving functional requirements
  - trend to loosely coupled
  - requirements for integration across diverse systems
- Assist with product selection and integration with respect to rapidly changing security product world

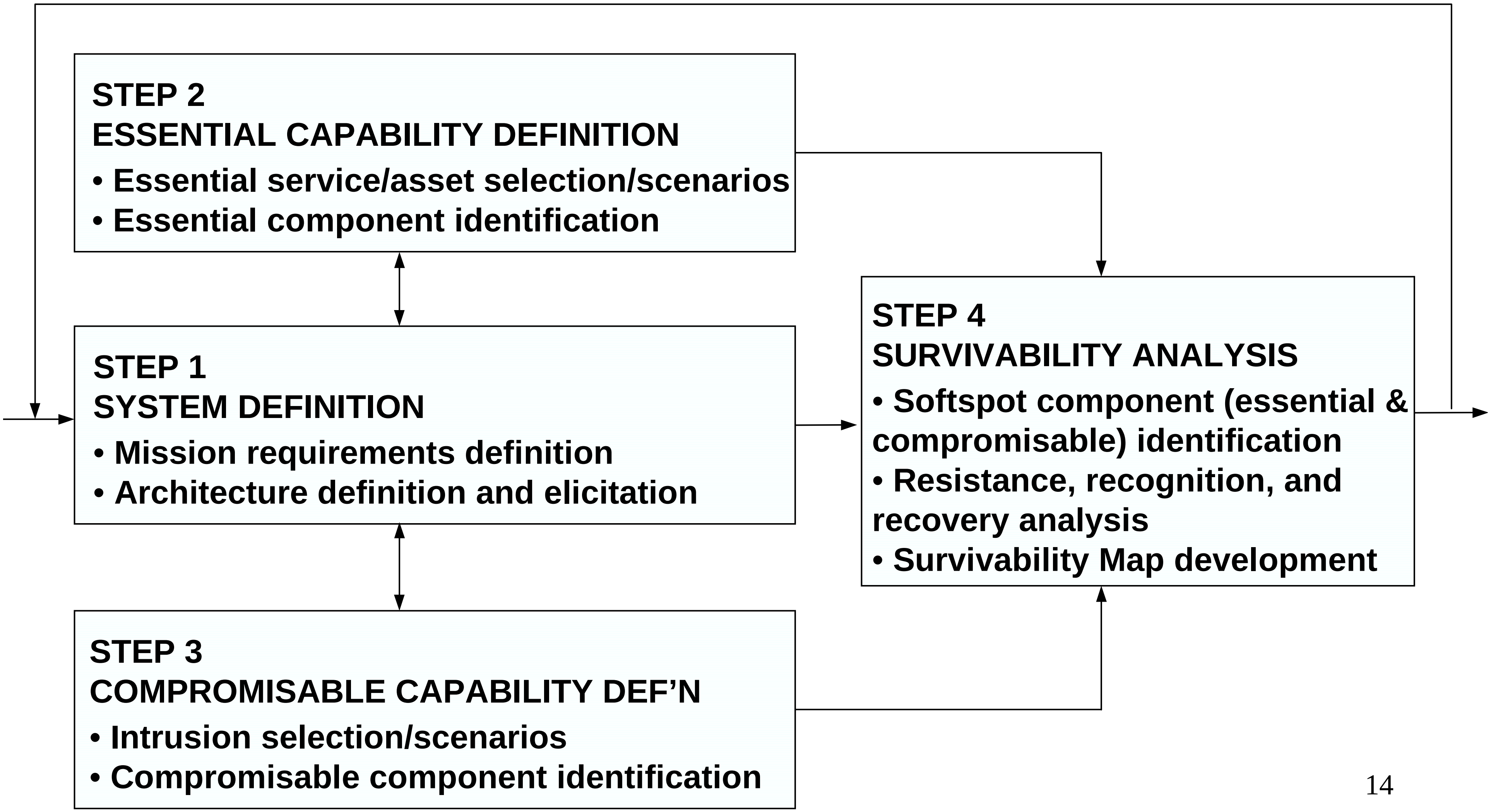
General Method

- Identify essential services with normal usage.
- Generate intrusion scenarios which are use cases for intruder
- Evaluate system in terms of response to scenarios
  - Requirements: propose response to intrusions
  - Architecture: evaluate system and operational behavior
- Mission impact
  - applications as well as system components
  - stakeholders input essential

Survivability Architecture

- Make recommendations for survivability improvements
- Identify decision and tradeoff points - areas of high risk
- Identify trade-offs with other software quality attributes
  - safety, reliability, performance, usability

The Survivable Network Analysis Method



STEP 2
ESSENTIAL CAPABILITY DEFINITION

- Essential service/asset selection/scenarios
- Essential component identification

STEP 1
SYSTEM DEFINITION

- Mission requirements definition
- Architecture definition and elicitation

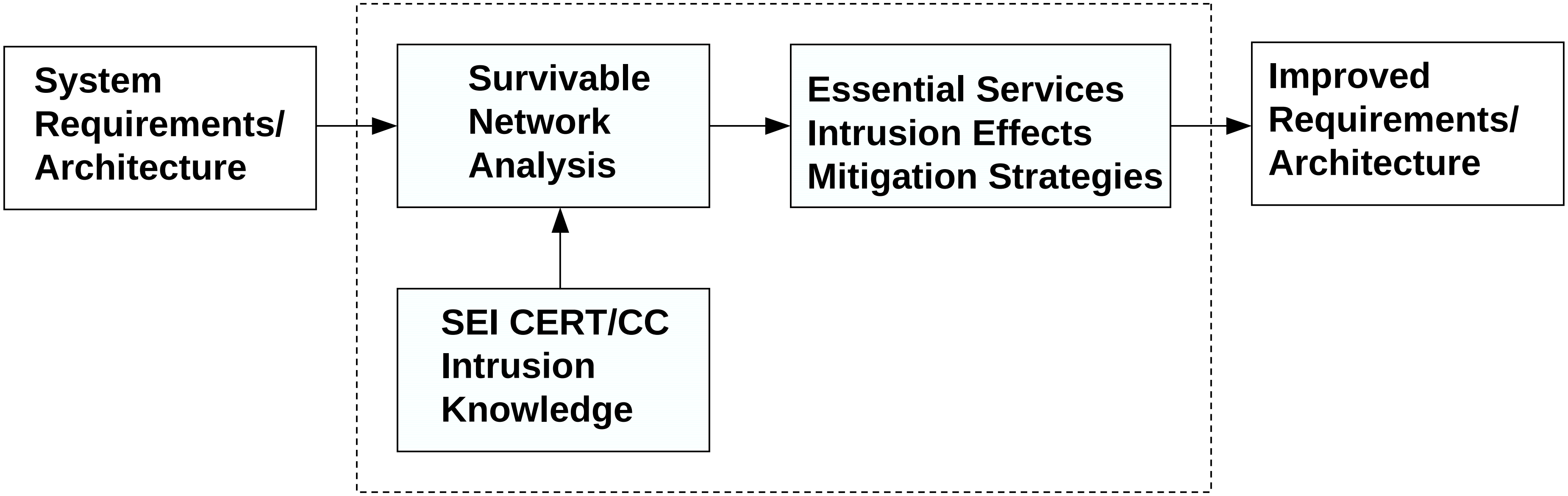
STEP 3
COMPROMISABLE CAPABILITY DEF’N

- Intrusion selection/scenarios
- Compromisable component identification

STEP 4
SURVIVABILITY ANALYSIS

- Softspot component (essential & compromisable) identification
- Resistance, recognition, and recovery analysis
- Survivability Map development

Determining Survivability Strategies


System Requirements/ Architecture
Survivable Network Analysis
Essential Services Intrusion Effects Mitigation Strategies
Improved Requirements/ Architecture
SEI CERT/CC Intrusion Knowledge

Survivability Map

Intrusion Scenario	Softspot Effects	Architecture Strategies for □	Resistance	Recognition	Recovery
(Scenario 1) …		Current			
		Recommended			
(Scenario n)		Current			
		Recommended			

- Roadmap for management evaluation and action

Option: Survivability Requirements

- Identify requirements for mission-critical functionality
  - minimum essential services
  - graceful degradation of services
  - restoration of full services

- Identify explicit requirements for
  - recovery
  - recognition
  - resistance

Option: Mission Lifecycle

- Factor survivability into the development and operational lifecycle
- Capture security and survivability assumptions
  - boundaries, users
- Identify survivability decision points
  - impact of changes on recovery, intrusion detection, etc.

Benefits of the SNA

- Clarified requirements
- Documented basis for system decisions
- Basis to evaluate changes in architecture
- Early problem identification
- Increased stakeholder communication

Additional Information

- SNA Case Study: The Vigilant Healthcare System
  - IEEE Software: July/August 1999
- Survivability: Protection Your Critical Systems
  - IEEE Internet Computing: Nov/December 1999
- Web site: IEEE article and other reports

  www.sei.cmu.edu/organization/programs/nss/surv-net-tech.html